FORCEPOINT KİMDİR?

Forcepoint, siber güvenlik alanında günümüzün en önemli riski olan kritik veriler ve fikri mülkiyet hakları ile etkileşim halinde olan kullanıcıların davranışlarını anlama konusuna odaklanarak siber güvenlik anlayışını bir sonraki nesline dönüştürmektedir.

Forcepoint şirketi 2016 yılında Websense'in kullanıcı koruması, veri güvenliği ve bulut uzmanlığı, Raytheon Cyber Products'ın iç tehdit ve analiz teknolojisi, Stonesoft'un yeni nesil güvenlik duvarı(NGFW) kabiliyetlerinin bir kombinasyonu olarak ortaya çıkmıştır. Son olarak şu anda Forcepoint CASB (Bulut Erişimi Güvenlik Aracısı) adını verdiğimiz Skyfence'in bulut uygulama koruması ve görünürlüğünü çözümünü de Şubat 2017 tarihinde bünyesine katmıştır. Bu sayede, Forcepoint, her sektörden Fortune 100 şirketlerinden orta ölçekli işletmelere ve dünyanın en güvenli savunma, istihbarat ve emniyet teşkilatlarına kadar çeşitli kuruluşları korumak için siber güvenliğin pek çok alanında uzun yıllara dayanan deneyimlerini birleştirmektedir. Bu dört işletme, her sektörden Fortune 100 şirketlerinden orta ölçekli işletmelere ve dünyanın en güvenli savunma, istihbarat ve emniyet teşkilatlarına kadar çeşitli kuruluşları korumak için siber güvenliğin pek çok alanında uzun yıllara dayanan deneyimlerini birleştirmektedir.

GÜVENLİK YAKLAŞIMIMIZ

BULUT GÜVENLİĞİ

Web Güvenliği

E-posta Güvenliği

Bulut Kum Havuzu (Sandboxing)

Bulut Erişim Güvenliği Aracısı (CASB)

AĞ GÜVENLİĞİ

Yeni Nesil Güvenlik Duvarı(NGFW)

VERİ VE İÇ TEHDİT GÜVENLİĞİ

İç Tehdit Koruması DLP

KÜRESEL HÜKÜMETLER

Alanlar Arası Çözümler

PROTECTING THE HUMAN POINT

NEDEN FORCEPOINT?

TANINMIŞ BİR SEKTÖREL TEKNOLOJİ LİDERİ

Gartner

2017 Kurumsal Veri Kaybı Koruması Magic Quadrant: Liderler Listesi

2017 Kurumsal DLP için Kritik Kabiliyetler: En Yüksek Ürün Puanı - Mevzuata Uyum Kullanım Senaryosu

IDC Analyze the Future

2016 IDC MarketScape: Dünya Çapında Web Güvenliği: Lider

2016 IDCMarketScape: Dünya Çapında E-posta Güvenliği: Lider

2016 IDC MarketScape SaaS E-posta Güvenliği: Lider

2016 IDC MarketScape: Donanım E-posta Güvenliği: Lider

SC MAGAZINE AWARDS

2015 En İyi Web İçeriği Yönetim Çözümü

2015 En İyi DLP Çözümü-EMEA

2015 SureView İç Tehdit Analizi

FORRESTER®

2016 Forrester Wave: Veri Kaybı Önleme Paketleri: Lider

2015 Forrester Wave: SaaS Web İçerik Güvenliği Wave: Lider

NSS LABS

2016 NSS Labs Tavsiyesi: Yeni Nesil Güvenlik Duvarı (NGFW)

2016 NSS Labs Tavsiyesi: Yeni Nesil IPS

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

2017 APT Koruması Market Quadrant Baş Aktör

2016 APT Koruması Market Quadrant Baş Aktör

2016 Kurumsal Web Güvenliği: Market Quadrant Baş Aktör

2016 Güvenli E-posta Ağ Geçidi (Secure E-mail Gateway) Market Quadrant Baş Aktör

FORCEPOINT
POWERED BY Raytheon

Küresel İş Ortağı Programı

GÜÇ • YENİLİK • BÜYÜME

E-POSTA GÜVENLİĞİ

E-posta Kaynaklı Tehditleri Önceden Durdurun

Forcepoint E-posta Güvenliği, istenmeyen e-posta ve kimlik avı e-postalarını (fidye yazılımı ve diğer gelişmiş tehditleri içeren), sistemlere kötü amaçlı yazılımları bulaştırmadan durdurur. Sektörün en güvenli bulut altyapısı üzerinde çalışan Forcepoint E-posta Güvenliği, Microsoft Office 365 ve diğer popüler e-posta sistemleri için emsalsiz kimlik avı, kötü amaçlı yazılım ve DLP koruması sunmaktadır.

Yeterlilik Soruları

- Fidye yazılımı ve diğer kimlik avı saldırılarının kuruluşunuza ne gibi etkileri vardır?
- Şu anda hassas konularda görüşme ve işbirliği yapmak için e-posta yazışmalarınızda nasıl bir şifreleme kullanıyorsunuz?
- Şu anda Office 365 Exchange Online kullanıyor musunuz veya bu programa geçmeyi planlıyor musunuz?

Kilit İş Değerleri

- Riski azaltır
- Uyumu kolaylaştırır
- İş verimliliğini artırır

BULUT ERİŞİM GÜVENLİĞİ ARACISI (CASB)

Bulutla Tanışın

Forcepoint CASB (bulut erişimi güvenlik aracısı), bulut uygulamalarında görünürlük ve kontrol sağlayarak kurum, güvenlik ve uyumla ilgili kör noktaları ortadan kaldırmaya yardımcı olur. Forcepoint CASB, onaylanmamış bulut uygulamalarının kullanımını keşfetme ve bununla ilgili riski değerlendirme imkanı sunar. Forcepoint CASB, onaylanmış bulut uygulamalarının (örneğin Office 365, Google Suite, Salesforce, Box, Dropbox, Workday) kritik fikri mülkiyeti korumak amacıyla nasıl kullanıldığını kontrol edebilir.

Yeterlilik Soruları

- Bulut uygulamalarınızın teşhir olmasından endişe duyuyor musunuz?
- Verilerin bulut yoluyla yayılması veya sızdırılmasından endişe duyuyor musunuz?
- Office 365, Box, Dropbox, Salesforce, Workday gibi uygulamaları kullanıyor musunuz veya kullanmayı planlıyor musunuz?

Kilit İş Değerleri

- Her yerdeki her bir kullanıcıyı koru
- Kör noktaları ortadan kaldır
- Bulut uygulamalarına uyum sağlayan güvenliği kullan

WEB GÜVENLİĞİ

Çalışanlarınızı Her Yerde Koruyun

Forcepoint Güvenli Web Ağ Geçidi'nin bulut tabanlı veya hibrit versiyonu olan Forcepoint Web Güvenliği, sektör lideri raporlama, kum havuzu (sandboxing) ve DLP kabiliyetleri sunar ve gelişmiş tehditlerin içeri girmesini ve hassas verilerin dışarı çıkmasını engeller. Forcepoint Web Güvenliği, verileri her yerde (bulutta, yolda ve ofiste) koruyarak, uyumu kolaylaştıran ve daha etkin bir güvenlik ortamında daha iyi kararlar alınmasını sağlayan birleşik bir platformun üzerine inşa edilmiştir.

Yeterlilik Soruları

- Dünyanın neresinde olursa olsun, ofis içinde ve dışındaki tüm son kullanıcıları korumak istiyor musunuz?
- Antivirüs korumasından, imza tabanlı olmayan gelişmiş tehditlere karşı gerçek zamanlı koruma sağlayan bir platforma geçmek istiyor musunuz?
- Bir fidye yazılımı saldırısının kurbanı oldunuz mu?

Kilit İş Değerleri

- Her yerdeki her bir kullanıcıyı koru (Direct Connect teknolojisi ile)
- Gelişmiş, koordine web ve e-posta saldırılarını önle
- Veri kaybını engelle

AĞ GÜVENLİĞİ

Bağla ve Koru

Forcepoint NGFW, insanları birbirine bağlar ayrıca ofisleriniz, şubeleriniz ve bulutta kullandıkları verileri en yüksek etkinlik, bulunabilirlik ve güvenlik seviyesinde korur.

Yeterlilik Soruları

- Ekipleriniz yeni sistemler kurmak ve bunları sürdürmek için ne kadar çaba harcamak zorunda kalıyor?
- Yeni uzak/şube tesislerini eklerken pahalı olmayan geniş bant hatlar mı yoksa yüksek fiyatlı özel hatlar mı kullanıyorsunuz?
- Artan şifrelenmiş trafiği denetlerken gizliliğe de önem veriyor musunuz?

Kilit İş Değerleri

- İş verimliliğini artırır
- Toplam Sahip Olma Maliyeti yüklerini azaltır
- Riski azaltır

İÇ TEHDİT

Kullanıcı Davranışı ve Firki Mülkiyet için Rakipsiz Görünürlük

Forcepoint İç Tehdit Çözümü, kendi kurumunuz içinden gelen, fikri mülkiyet ve mevzuata uyum konusunda risk teşkil eden tehditlere karşı erken uyarı sağlar. Forcepoint İç Tehdit Çözümü, herhangi bir kullanıcının eylemlerinin bağlamını göstermek için video kaydı ve video tekrarı özelliklerinin kullanımı sayesinde güvenlik ekiplerinin ele geçirilmiş kullanıcılar, şirket içindeki kötü niyetli kişiler ve yanlışlıkla yapılan davranışları ayırt etmesini sağlar.

Yeterlilik Soruları

- Riskli olabilecek şekilde davranan kullanıcıları nasıl belirlersiniz?
- Şüpheli davranışları fikri mülkiyet veya düzenlenmiş verileriniz için bir tehdit haline gelmeden önce tespit edebilir misiniz?
- Bir olayın kötü niyetli kullanıcı, kaza veya ele geçirilen hesaptan mı kaynaklandığını nasıl anlarsınız?

Kilit İş Değerleri

- Risk puanı oluşturmak için davranış analizlerini kullan
- Kullanıcı davranışlarına bakarak en riskli kullanıcıları otomatik olarak tespit et
- Davranışların yorumlanması ve gerekirse takibat için forensic araçlar sağla

DLP

Yüksek Görünürlük ve Veri Kontrolü Sağlayın

Gartner tarafından mevzuata uyum konusunda lider olarak değerlendirilen Forcepoint DLP, en büyük riski oluşturan veri olaylarını otomatik olarak tespit etmek için sektörün en yenilikçi DLP teknolojilerini (Güvenlik Analizi dahil) sunmaktadır. Forcepoint DLP, kullanıcı davranışına yönelik görünürlük sağlamak için davranış analizi ve Olay Riski Sıralaması (IRR) panosu sunan tek DLP sağlayıcısıdır.

Yeterlilik Soruları

- Kuruluşunuza gelen veya kuruluşunuzdan çıkan düzenlenmiş veriler ve IP için görünürlük söz konusu mu?
- Kurumsal ağ dışındaki uç noktalarda bulunan verileri nasıl koruyorsunuz? Mac bilgisayarlarınızı nasıl koruyorsunuz?
- Hangi bulut uygulamalarını kullanıyorsunuz? 0365, Box ve Google Drive gibi bulut uygulamalarında bulunan verilerin güvenliğini nasıl sağlıyorsunuz?

Kilit İş Değerleri

- Şirket içi, uç noktalar ve bulut uygulamalarındaki veriler için görünürlük ve koruma
- Alarm durumu aşırı yükünü kolaylaştırır
- Ağ dışı uç noktalardan kaynaklanan veri kaybı riskini azaltın

İLETİŞİM

partner@forcepoint.com @Forcepointsec www.forcepoint.com